Microsoft

Microsoft Windows

Common Criteria Evaluation

Microsoft Windows 8

Microsoft Windows Server 2012

Microsoft Windows 8, Microsoft Windows Server 2012 Common Criteria Supplemental Admin Guidance for Software Full Disk Encryption

DOCUMENT INFORMATION

Version Number	1.0
Updated On	April 3, 2014

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

1 Version Information

Specification Filename	Administrative Guidance for Software Full Disk Encryption Clients
Specification version, date	1.0, April 3, 2014

2 Preparing to Use BitLocker

This document provides administrative guidance to configure and use BitLocker for full disk encryption. Except as specifically noted all management procedures described in this document require the user to provide administrator credentials.

Once BitLocker is configured by the administrator then disk volumes are encrypted and decrypted without user intervention. However, if BitLocker is configured to use an authorization factor that requires an input, such as a PIN or password, the authorization factor must be provided before the disk is unlocked.

Users should not leave the computer unattended when it is in a mode while there is user data in volatile memory. In those cases, the user should either shut down the computer or place it into a hibernation state (the ACPI S4 state) instead of leaving the machine in the working state (ACPI S0 state). The powercfg.exe utility manages the power and hibernation settings for the computer.

Users should also realize that computers which support Connected Standby, which are primarily tablets, convertibles, and ultrabooks, the computer will always operate in the S0 state unless they shut the computer down from the Windows logon/logoff screen or hibernate the machine. In the same manner as a smartphone, pressing the power button places the machine into standby.Users must not leave or store the PINs, passphrases, and external token authorization factors in the same location.

2.1 Supported Windows Editions

BitLocker is supported on Windows Server 2012 Standard and Datacenter editions, Windows 8 Pro and Enterprise 32-bit and 64-bit editions. BitLocker provides identical support on the Windows 8 and Windows Server 2012 editions.

2.2 Before Starting

The following TechNet articles are a useful introduction to BitLocker:

- BitLocker Overview: http://technet.microsoft.com/en-US/library/hh831713.aspx[1]
- BitLocker Frequently Asked Questions (FAQ): http://technet.microsoft.com/en-us/library/hh831507.aspx[2]

[1] The Encrypted Hard Drive feature is not included in this evaluation.
[2] Since the BitLocker volume is unlocked automatically when BitLocker is suspended, administrators should not take any action that will suspend BitLocker protection.

- Prepare your organization for BitLocker: Planning and Policies: http://technet.microsoft.com/en-us/library/jj592683.aspx

3 Deploying BitLocker

To maintain compliance with the Full Disk Encryption Security Target all the physical and logical drives for a given computer must be encrypted using BitLocker. However, some computers have system partitions that are not visible by default to users, such as a system recovery partition for restoring the factory default state. These partitions should not be modified in a way that can directly store user data or encrypted using BitLocker.

In order to ensure continuous,uninterrupted protection, the administrator should never suspend BitLocker after the disk volume has been encrypted unless the administrator is prepared for the computer to operate out of the evaluated configuration. For example, if it is necessary to change the UEFI or BIOS configuration on computers with BitLocker volumes enabled, you should first suspend BitLocker.

3.1 Installing BitLocker for Windows 8

BitLocker is installed by default on the evaluated Windows 8 editions.

3.2 Installing BitLocker for Windows Server 2012

BitLocker is not installed by default on Windows Server 2012.This TechNet article describes how to install BitLocker using Server Manager or PowerShell commands:

- BitLocker: How to deploy on Windows Server 2012: http://technet.microsoft.com/en-us/library/jj612864.aspx

3.3 Using Authorization Factors

BitLocker includes the capability for using multiple authorization factors that must be provided before unlocking, i.e., providing access to the encrypted data, the encrypted operating system drive and other encrypted disk volumes. Authorization factors can be used by themselves or can be combined for multiple factor authorization. Authorization factors are used to protect the Full Volume Encryption Key (FVEK) that encrypts the disk volume and are also referred to as “key protectors”. The authorization factors are (bold items are included in the evaluated configuration):

- TPM
  Stores the authorization factor on the TPM and automatically retrieves it to unlock the operating system volume.

- TPM and Personal Identification Number (PIN)
  Require the user to enter a numeric PIN before automatically retrieving the key protector from the TPM to unlock the operating system volume.

- TPM and Enhanced PIN
  Require the user to enter an alphanumeric PIN before automatically retrieving the key protector from the TPM to unlock the operating system volume.

- **TPM and Startup Key**
  Require the user to insert a USB drive containing the Startup Key for decryption before automatically retrieving the key protector from the TPM to unlock the operating system volume.

- **TPM and PIN and Startup Key**
  Require the user to enter a PIN and to insert a USB drive containing the Startup Key before automatically retrieving the key protector from the TPM to unlock the operating system volume.

- **TPM and Enhanced PIN and Startup Key**
  Require the user to enter an Enhanced PIN and to insert a USB drive containing the Startup Key before automatically retrieving the key protector from the TPM to unlock the operating system volume.

- **Startup Key**
  Require the user to insert a USB drive containing the Startup Key to unlock the volume.

- **Recovery Key**
  Require the user to enter the recovery key to unlock the volume.

- **Password**
  Require the user to enter the password to unlock the volume.

- Recovery Password
  Require the user to enter the recovery password to unlock the volume.

3.4 Options to use a single authorization factor or multiple authorization with the manage-bde command is described in the Using BitLocker without a Compatible TPM

To enable BitLocker for the operating system volume on a computer without a compatible TPM do the following:

1. As an administrator, start the gpedit.msc MMC snap-in
2. In the left pane navigate to **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives**
3. Open the **Require additional authentication at startup** policy, select the **Enabled** radio button and then select the **Allow BitLocker without a compatible TPM** check box

After this setting is applied the non-TPM settings appear in the BitLocker setup wizard or the manage-bde command-line utilty can be used to enable BitLocker for the operating system volume.

Note: This policy must also be set on a computer with a compatible TPM in order to enable BitLocker on an operating system disk drive without also using a TPM authorization factor.

Enabling BitLocker section.

Authorization factors can also be managed after encryption is enabled. These TechNet articles describe how to use the **manage-bde** or **Add-BitLockerKeyProtector** and **Remove-BitLockerKeyProtector** PowerShell cmdlets to add additional or manage existing authorization factors:

- Manage-bde: protectors: http://technet.microsoft.com/en-us/library/ff829848(v=ws.10).aspx
- Add-BitLockerKeyProtector: http://technet.microsoft.com/en-us/library/jj649835.aspx
- Remove-BitLockerKeyProtector: http://technet.microsoft.com/en-us/library/jj649826.aspx

Group policy settings can be configured to require or disable specific authorization factors as described in the following TechNet article:

- BitLocker Group Policy settings: http://technet.microsoft.com/en-us/library/jj679890.aspx

3.5 Configuring Cipher Algorithms

AES 128 is the default encryption algorithm to encrypt disk volumes . The commands shown below for enabling BitLocker accept this default encryption strength. AES 256 encryption algorithm can also be used.

The following TechNet article explains how to choose the encryption algorithm. Options for setting the encryption strength are available when enabling encryption with the **manage-bde** command or the **enable-bitlocker** PowerShell cmdlet:

- Manage-bde: on (see the -encryptionMethod attribute): http://technet.microsoft.com/en-us/library/ff829873.aspx
- Enable-BitLocker: http://technet.microsoft.com/en-us/library/jj649837.aspx

The default encryption algorithm choice can also be configured in group policy for supported Windows 8 and Windows Server 2012 editions. The following TechNet article explains the group policy settings that control encryption cipher strength:

- http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_encryptmeth

To use the same configuration as in the Windows FIPS 140 validations, set the following policy in group policy (described further at http://support.microsoft.com/kb/811833).

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

Windows implements two random number generators the FIPS-140 validated AES CTR DRBG and the Dual EC DRBG. If there is a need to switch from the AES CTR DRBG follow the procedures at http://msdn.microsoft.com/en-us/library/aa375458(v=vs.85).aspx.

3.6 Using BitLocker without a Compatible TPM

To enable BitLocker for the operating system volume on a computer without a compatible TPM do the following:

4. As an administrator, start the gpedit.msc MMC snap-in
5. In the left pane navigate to **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives**
6. Open the **Require additional authentication at startup** policy, select the **Enabled** radio button and then select the **Allow BitLocker without a compatible TPM** check box

After this setting is applied the non-TPM settings appear in the BitLocker setup wizard or the manage-bde command-line utilty can be used to enable BitLocker for the operating system volume.

Note: This policy must also be set on a computer with a compatible TPM in order to enable BitLocker on an operating system disk drive without also using a TPM authorization factor.

3.7 Enabling BitLocker for Windows 8 and Windows Server 2012

The commands below should be executed in a command shell while running as an administrator. The manage-bde command is described in this TechNet article:

- Manage-bde: http://technet.microsoft.com/en-us/library/ff829849(v=ws.10).aspx

Some authorization factors are included as part of the evaluated configuration, while other combinations are excluded; the authorization factors which are used by the evaluated configuration are:

Authorization Factor	Unlocks	Part of evaluated configuration?
TPM	Operating System Drive	No
TPM + PIN	Operating System Drive	No
TPM + Start-up Key	Operating System Drive	Yes
TPM + PIN + Start-up Key	Operating System Drive	Yes
TPM + Enhanced PIN	Operating System Drive	No
TPM + Enhanced PIN + USB [Start-up Key]	Operating System Drive	Yes
External Key[3]	Operating System Drive and Data Volume	Yes
Recovery Password	Operating System Drive and Data Volume	No
Clear Key[4]	Operating System Drive	No

[3] This can be startup key or a recovery key.
[4] BitLocker generates the clear key when the administrator chooses to suspend BitLocker.

Passphrase	Data Volumes (and Windows To Go) and Operating System Drive	Yes
Public Key (RSA and ECDH)[5]	Data Volume	No

3.7.1 TPM

To enable the TPM authorization factor execute the following command:

```
Manage-bde –on <operating system disk volume letter>:
```

3.7.2 TPM and PIN

To enable the TPM and PIN authorization factors execute the following command:

```
Manage-bde –on <operating system disk volume letter>: -tpmandpin
```

Administrators must create a PIN value with a minimum of four and a maximum of 20 numeric characters.

3.7.3 TPM and Enhanced PIN

To enable the TPM and Enhanced PIN authorization factors execute the following command:

```
Manage-bde –on <operating system disk volume letter>: -tpmandpin
```

Administrators must create an Enhanced PIN value with a minimum of four and a maximum of 20 numeric characters, but can also include uppercase and lowercase English letters, symbols on an EN-US keyboard, numbers, and spaces. To enable the Enhanced PIN capabilities start the gpedit.msc MMC snap-in as an administrator and enable the following local or group policy:

- **Administrative Templates\Windows Components\Bitlocker Drive Encryption\Operating System Drives\Allow enhanced PINs for startup**

3.7.4 TPM and Startup Key

To enable the TPM and startup key authorization factors execute the following command:

```
Manage-bde –on <operating system disk volume letter>: -tpmandstartupkey <USB
volume letter for startup key>:\
```

Note the startup key is created as a hidden, system file named as <startup key GUID>.BEK.

USB disks that hold startup keys must not be used for any other purpose.

3.7.5 TPM and PIN and Startup Key

To enable the TPM and PIN and Startup Key authorization factors execute the following cmdlet in a PowerShell running as administrator:

```
Enable-bitlocker –mountpoint <operating system disk volume letter to
encrypt>: -startupkeypath <USB volume letter for startup key>:\
-tpmandpinandstartupkey
```

Note the startup key is created as a hidden, system file named as <startup key GUID>.BEK.

The **enable-bitlocker** cmdlet is documented in the following TechNet article:

- **Enable-BitLocker**: http://technet.microsoft.com/en-us/library/jj649837.aspx

Note: In some cases when the startupkey is corrupted the error message displayed may incorrectly indicate that an incorrect PIN has been entered.

USB disks that hold startup keys must not be used for any other purpose.

3.7.6 TPM and Enhanced PIN and Startup Key

To enable the TPM and Enhanced PIN and Startup Key authorization factors execute the following cmdlet in a PowerShell running as administrator:

```
Enable-bitlocker –mountpoint <operating system disk volume letter to
encrypt>: -startupkeypath <USB volume letter for startup key>:\ -
tpmandpinandstartupkey
```

Note the startup key is created as a hidden, system file named as <startup key GUID>.BEK.

The **enable-bitlocker** cmdlet is documented in the following TechNet article:

- **Enable-BitLocker**: http://technet.microsoft.com/en-us/library/jj649837.aspx

Administrators must create an Enhanced PIN value with a minimum of four and a maximum of 20 numeric characters, but can also include uppercase and lowercase English letters, symbols on an EN-US keyboard, numbers, and spaces. To enable the Enhanced PIN capabilities start the gpedit.msc MMC snap-in as an Administrator and enable the following local or group policy:

- **Administrative Templates\Windows Components\Bitlocker Drive Encryption\Operating System Drives\Allow enhanced PINs for startup**

In If the startupkey is corrupted the error message displayed may claim that an incorrect PIN has been entered.

USB disks that hold startup keys are not to be used for any other purpose.

3.7.7 Startup Key

To enable the startup key authorization factor execute the following command:

```
Manage-bde –on <disk volume letter to encrypt>: –startupkey <USB volume
letter for startup key>:\
```

If the computer has a TPM, then the TPM authorization factor is automatically added so that TPM or startup key can be used to unlock the volume. To enable only the startup key authorization factor the TPM authorization factor can be removed with the following command:

```
Manage-bde c: -protectors –delete -type tpm
```

Note the startup key is created as a hidden, system file named as <startup key GUID>.BEK.

USB disks that hold startup keys must not be used for any other purpose.

3.7.8 Recovery Key

A recovery key is used to recover an encrypted disk volume protected by authorization factors that are not available. To create a Recovery Key authorization factor execute the following command:

```
Manage-bde –on <disk volume letter to encrypt>: –recoverykey <USB volume
letter for recovery key>:\
```

This command will also automatically enable the TPM authorization factor if the recovery key is being created for the operating system volume and a TPM authorization factor is being used. A recovery key can also be added after BitLocker is already enabled for a given disk volume by using the following command:

```
Manage-bde <disk volume letter>: -protectors –add –RecoveryKey <USB volume
letter for recovery key>:\
```

Note the recovery key is created as a hidden, system file named as <recovery key GUID>.BEK. recovery keys and startup keys are also referred to as external keys and are effectively identical in use.

USB disks that hold recovery keys must not be used for any other purpose.

On a Surface Pro computer when using a recovery (or start up) key to unlock the operating system disk,the volume down button which is located on the side of the tablet must be pressed down during boot to allow the computer to enumerate the USB drives and then find the recovery key.

3.7.9 Password

To enable the password authorization factor execute the following command:

```
Manage-bde –on <disk volume letter to encrypt>: –password
```

The command prompts the user for the password and then prompts the user to confirm the password. Administrators must create password values that use a minimum of 64 characters. The allowed set of characters are upper and lower English letters, the digits 0 – 9, and the following symbols: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”.

The password authorization factor cannot be used to enable BitLocker on an operating system disk drive without a TPM authorization factor unless the **Allow BitLocker without a compatible TPM** policy is set as shown in section Using BitLocker without a Compatible TPM.

3.7.10 Recovery Password

The recovery password authorization factor, which is not supported by the evaluated configiatuion and should not be used, would be enabled by this command:

```
Manage-bde –on <disk volume letter to encrypt>: –recoverypassword
```

3.8 Disabling BitLocker

BitLocker is turned off and will decrypt a disk volume after one or more authorization factors have been provided by starting a command shell as administrator and executing the following command:

```
Manage-bde <encrypted disk volume letter>: -off
```

3.9 Verifying Disk Volume Encryption State

The encryption status of a disk volume can be cheked by starting a command shell as administrator and executing the following command:

```
Manage-bde <encrypted disk volume letter>: -status
```

3.10 Locking Data Volumes

A data volume is locked, i.e., will require an authorization factor to access the encrypted data, by starting a command shell as administrator and executing the following:

```
Manage-bde –lock <encrypted data disk volume letter>:
```

3.11 Unlocking Data Volumes

A fixed data volume is unlocked by starting a command shell as Administrator and executing the following command for the case of an recovery key authorization factor for a fixed disk:

```
Manage-bde –unlock <encrypted fixed data disk volume letter>: -recoverykey
<pathname to recovery key file>
```

The Windows Explorer user interface must be used to unlock encrypted removable disk volumes for the case of recovery key.

For password authorization factors the administrator can use the following commands for either fixed or removable data disk volumes:

```
Manage-bde –unlock <encrypted data disk volume letter>: -password <password>
```

Note that the online documentation does not include the `–password` option, however `manage-bde –unlock –help` lists the `–password` option and other authorization factors.

A standard user or administrator user unlocks a data disk volume by starting the Windows Explorer application, clicking the **Computer** node in the left pane, and then clicking **Unlock drive** for the indicated fixed or removable disk drive. Depending upon the type of authorization factors that are enabled for the data disk volume, the user will be prompted to load the key from a USB drive, provide the Password, Recovery Password or Recovery Key, or to insert a Smart Card.

4 Changing Authorization Data

This section discusses how to change the authorization data for the authorization factors that protect an encrypted volume. The commands shown in this section should be executed in a command shell running as administrator.

4.1 TPM and PIN

The PIN value for the TPM and PIN authorization factor is changed by executing the following command:

```
Manage-bde –changepin <encrypted operating system disk volume letter>:
```

The command prompts for a new PIN and confirms the new PIN. After the changepin operation completes successfully the old PIN is no longer valid and the new PIN is now the current PIN.

4.2 Startup Key

The value for a startup key authorization factor for an operating system volume is changed by executing the following command:

```
Manage-bde –changekey <encrypted operating system volume letter>: <USB volume
letter for startup key>:\
```

Since the volume will already be unlocked the current startup key need not be present (e.g. the USB volume containing the current startup key need not be inserted). If the `changekey` command completes successfully, then the new startup key becomes the current startup key and the old startup key can no longer be used to unlock the encrypted disk volume.

The `changekey` command cannot be used for data volumes. To change the startup key for a data volume the current startup key must be removed and then a new startup key added. If the current startup key is the only key protector for the data volume, then a password key protector could be added for the startup changekey operation in order to ensure a key protector is present at all times on the data volume.

4.3 Password

The value for a password authorization factor is changed by executing the following command:

```
Manage-bde –changepassword <encrypted disk volume letter>:
```

The command prompts the user for the new password. After the change password operation completes successfully the old password is no longer valid and the new password becomes the current password.

Administrators must create password values that use a minimum of nine words with no word longer than eight characters. The allowed sets of characters are upper and lower English letters, the digits 0 – 9, and the following symbols: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”.

If the password authorization factor is the only authorization factor on an operating system disk then changing the password will fail with an error indicating that the last protector may not be deleted. However a second authorization factor may be added to the disk. Once a second authorization factor is

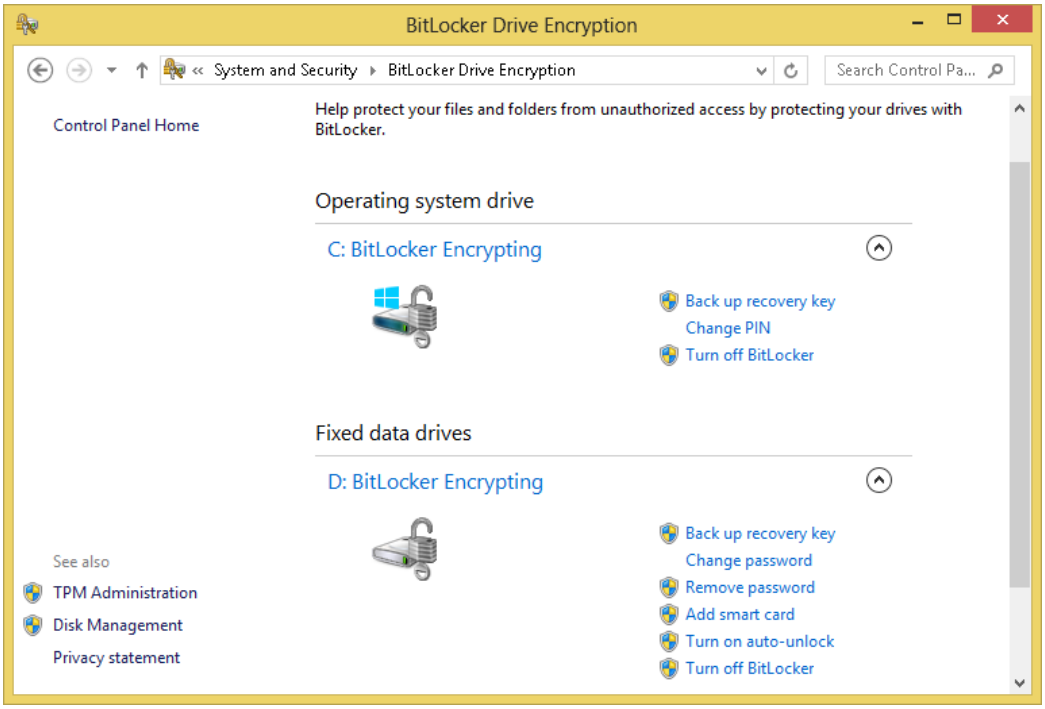
added then changing the password will succeed. Once the password is changed then the second authorization factor may be removed.

4.4 Changing PIN or Password as a Standard User

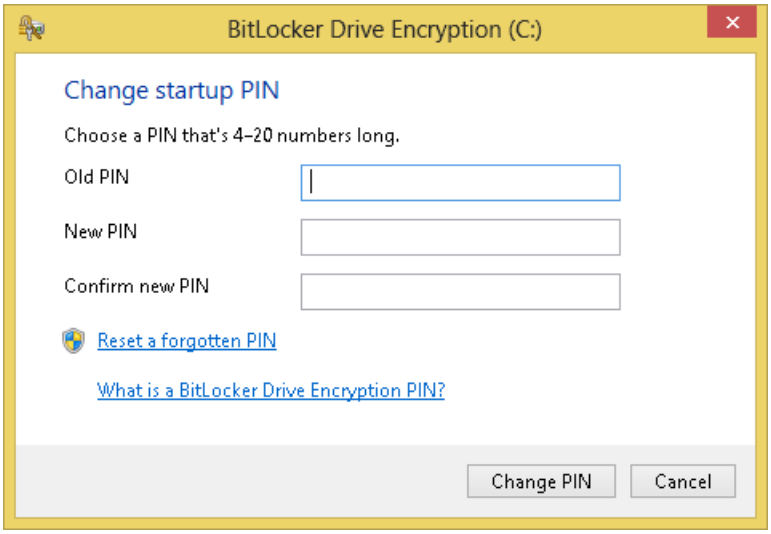
While administrator credentials must be provided to execute the **manage-bde** command, a standard user can change the TPM PIN or the password authorization factors without providing administrator credentials by using the BitLocker Control Panel.

1. Click **Start**, type “Control Panel” and click “Control Panel” in the search results. If Control Panel is displaying **View by: Category**, then click **System and Security**, and then click **BitLocker Drive Encryption**. Otherwise if it is displaying the icon view then click **BitLocker Drive Encryption**.

2. In the BitLocker Drive Encryption control panel, click **Change PIN** or **Change Password**. See the figure below:



3. To change the PIN, in the BitLocker Drive Encryption dialog enter the old PIN value and create the new PIN value. See figure below:



4. To change the password, in the BitLocker Drive Encryption dialog enter the old password value and create the new password value. Users must create new password values that use a minimum of nine words with no word longer than eight characters. The allowed sets of characters are upper and lower English letters, the digits 0 – 9, and the following symbols: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. See figure below:

Note: The Administrator should inform standard users of the password policy.

5 Changing the Full Volume Encryption Key

Should a user desire to change the key that encrypts the storage volume, then should turn off BitLocker and then turn it on again. This will decrypt the disk and then encrypt it again with a new key. This should be done only in the rarest of circumstances because decrypting the disk will leave the user data unprotected.

6 Using Key Recovery

Key recovery is used to unlock BitLocker-encrypted drives with a recovery key or a recovery password when the other key protectors can no longer be used. For example if a TPM key protector is invalidated by system changes, then a recovery password can unlock the operating system drive. It is important to consider that the recovery password was not part of the evaluated configuration and must not be used by organizations that need to operate BitLocker in the same manner as the evaluated configuration.

Recovery keys, however, are allowed to be used in the evaluated configuration if they are contained (solely) on a USB in the user's possession, and not archived to Active Directory nor archived to the users' Microsoft account.

6.1 Enabling Group Policy for Key Recovery

Group policy settings can be enabled to require creating recovery protectors when enabling BitLocker for an operating system, fixed or removable drive. In addition, group policy can be used to store the recovery password or recovery keyin Active Directory; this capability should not be used by organizations that are required to operating within the evaluated configuration. The following Technet article describes how to manage these policies:

- Scenario 8: Specifying How BitLocker-Protected Drives Can Be Recovered (Windows 7): http://technet.microsoft.com/en-us/library/ee424303(v=ws.10).aspx[6]

The administrator should not select the **Allow data recovery agent** option for the **Choose how BitLocker-protected operating system drives can be recovered** group policy setting.

6.2 Recovering a BitLocker-encrypted Drive

Users can recover a BitLocker-encrypted drive with a recovery protector by following the instructions in the following Technet article:

- Scenario 11: Recovering Data Protected by BitLocker Drive Encryption (Windows 7): http://technet.microsoft.com/en-us/library/ee424308(v=ws.10).aspx

Using a recovery key that is stored on a USB drive will eliminate the need to use a recovery password when recovering an encrypted storage volume.

7 Disabling the Sleep Power States

The “Power management Group Policy settings” heading in the following TechNet topic describes how to disable the sleep power states in support of the power management function described in the security target:

- BitLocker Group Policy settings: http://technet.microsoft.com/en-us/library/jj679890.aspx

[6] This article also applies to Windows 8 and Windows Server 2012.

Should a user need to enable the hibernation ACPI power state (S4), instead of relying on the Connected Standby operations in ACPI power state (S0), they can use **powercfg.exe** to manage the ACPI power state.

8 Disabling Authorization Data Backup to Active Directory

The TOE must not allow BitLocker authorization factors to be copied to Active Directory for escrow. The following TechNet topic describes how to disable this feature local or group policy:

- "Backing Up BitLocker and TPM Recovery Information to AD DS": http://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx

Follow the instructions "Configure Group Policy to enable backup of BitLocker and TPM recovery information in AD DS" that are indicated as applying to Windows 7 and Windows Server 2008 R2, which also apply to Windows 8 and Windows Server 2012, to disable rather than enable the policies.

9 Disabling Recovery Keys and Recovery Passwords

9.1 Windows 8 and Windows Server 2012

Use of the recovery key and recovery password authorization factors can be disabled by local or group policy by starting the gpedit.msc MMC snap-in as administrator and conducting the following steps:

1. Navigate to **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption** in the left pane and double-click the item for the type of drive to be configured:
   Fixed Data Drives
   Operating System Drives
   Removable Data Drives
2. Double-click the **Choose how BitLocker-protected operating system drives can be recovered** policy
3. Click the **Enabled** radio button
4. To disable the Recovery Password authorization factor select **Do not allow 48-digit recovery password** in the **Configure user storage of BitLocker recovery information** dropdown listbox
5. To disable the Recovery Key authorization factor select **Do not allow 256-bit recovery key** in the **Configure user storage of BitLocker recovery information** dropdown list
6. Click the **OK** button

To prevent a recovery password or recovery key authorization factor from being created for a given disk volume, the relevant recovery policy must be disabled before the disk volume is encrypted. Otherwise, if the disk volume was enabled for BitLocker before the policy was disabled, then the only way to prevent conducting a recovery operation on that disk volume is to turn off BitLocker on that disk volume. Doing so will invalidate any Recovery Passwords or Recovery Keys that were created for that disk volume. That

disk volume can then be reenabled for BitLocker with assurance that a recovery operation cannot be conducted since a recovery password or recovery key authorization factor cannot be created by policy.

If the organization does not use group policy to manage BitLocker authorization factors, note that the BitLocker control panel application will generate a recory password by default and the manage-bde.exe application will generate a recovery password if the –RecoveryPassword parameter is included in the command line.

10 Managing Product Updates

10.1 Updating Windows

Updates to Windows are delivered as Microsoft Update Standalone Package files (.msu files) and are signed by Microsoft with two digital signatures, a SHA1 signature for legacy applications and a SHA256 signature for modern applications. The SHA1 and SHA256 digital signatures are signed by *Microsoft Corporation*, with a certification path through a Microsoft Code Signing certificate and ultimately the Microsoft Root Certification Authority.

The Windows operating system will check that the certificate is valid and has not been revoked using a standard PKI.

Updates to Windows are delivered through the Windows Update capability, which is enabled by default, or the user can go to http://www.microsoft.com/security/default.aspx to search and obtain security updates on their own volition.

10.2 Verifying the TOE version

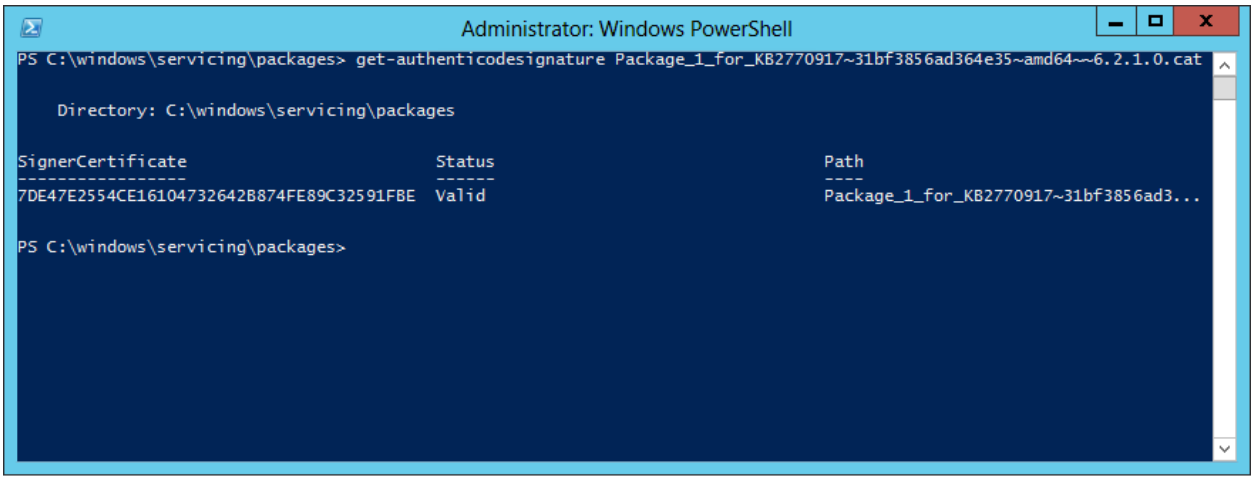
In order to verify the TOE version the following command can be executed at the command prompt to list the OS Name, OS Version and installed Hotfixes:

```
systeminfo
```

The OS Name, OS Version, and list of installed Hotfixes are listed.

10.3 Verifying Product Updates

Update packages downloaded by Windows Update are signed with the Microsoft Root Certificate Authority to prove their authenticity and integrity. This signature is verified by the Windows Update service before installing any of the product updates contained in a given package. The packages are stored in the folder c**:\windows\servicing\packages**. The package signatures may be independently verified by using the **Get-AuthenticodeSignature** PowerShell cmdlet as shown in the figure below for one of the updates for Windows 8 and Server 2012:



To obtain more information regarding a given update package (e.g. the files that will be updated from the package) go to http://support.microsoft.com/kb/XXX where XXX is the given KB number in the filename for the given package in **c:\windows\servicing\packages** or in the Windows Update listing of proposed packages to be installed on a given system (e.g. KB2770917 as shown in the figure above).